White Paper

CenturyLink Managed Security Services

Overcoming the Security Skills Gap

By Doug Cahill, ESG Senior Analyst and Tony Palmer, ESG Senior Lab Analyst
October 2016

This ESG White Paper was commissioned by CenturyLink
and is distributed under license from ESG.

Contents

Introduction

The challenge of keeping pace with the evolving threat landscape has been compounded by employee mobility and hybrid clouds, requiring organizations to adapt by investing in a contemporary set of tools, tactics, technologies, and skills to protect data assets from compromise and ensure business continuity. Research conducted by ESG highlights this imperative with surveyed participants citing cybersecurity initiatives as the top IT priority for 2016.[1] However, an acute shortage of cybersecurity skills is limiting the ability of many organizations to implement those initiatives. In fact, 46% of participants in the same research conducted by ESG indicated that they have a problematic shortage of cybersecurity skills (see Figure 1).

Figure 1. IT Skills Shortages

In which of the following areas do you believe your IT organization currently has a problematic shortage of existing skills? Which area has the most significant shortage of skills? (Percent of respondents, N=627)

Area	Percent
Cybersecurity	46%
Mobile application development	37%
Business intelligence/data analytics	36%
Social media/marketing technologies	34%
Enterprise mobility management	31%
Server virtualization/private cloud infrastructure	31%
Compliance management, monitoring and reporting	30%
Social enterprise/collaboration technologies	30%
IT architecture/planning	30%
Application development	28%

Source: Enterprise Strategy Group, 2016

This dichotomy of needing to protect against new threats with a deficit of the skills and resources required to do so puts security leaders in a position of needing to meet two potentially conflicting objectives: increasing threat prevention efficacy, while also increasing operational efficiency. In addition, customers are not getting full value out of the investments they have already made in cybersecurity technologies, particularly those that are complicated and require a high level of product-specific competency. Such "point-tool fatigue" is resulting in demand for platforms that integrate previously disparate technologies for streamlined workflows and shared services such as threat intelligence.
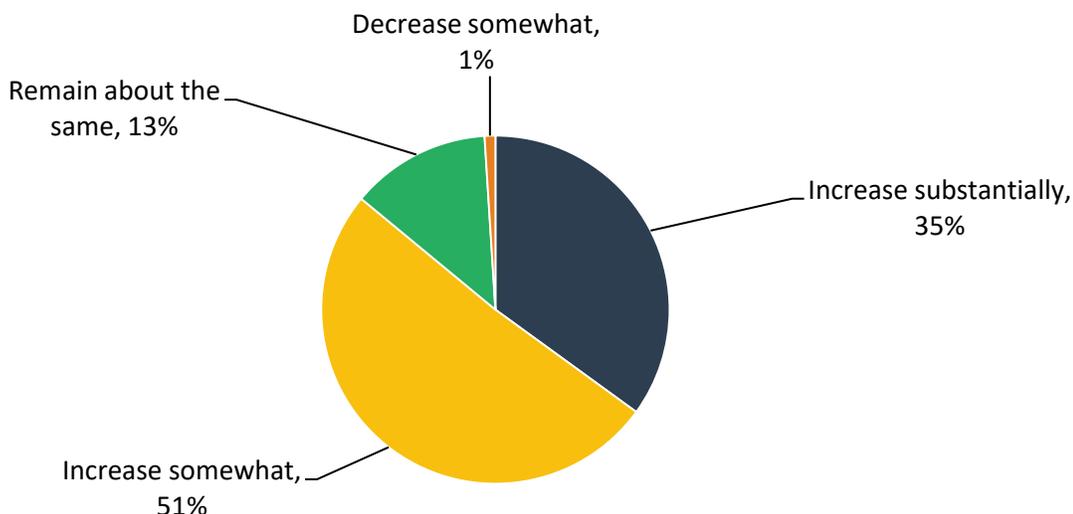
The Shift Toward Managed Security Services

The increased awareness of security breaches has made cybersecurity a business issue and thus a "team sport" characterized by increased collaboration among security, IT, and line-of-business personnel. To address the shortage of cybersecurity skills, that set of collaborators is expanding to include third-party organizations that can offer the resources, expertise, and services to augment and extend the internal IT and security teams. Managed security service providers

---

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

(MSSPs) are playing an increasingly relevant role, helping organizations secure their assets and infrastructure with both operational services and strategic engagements. While 42% of respondents in research conducted by ESG stated that they are already using an extensive set of managed security services, the research also highlights a notable expected increase in the use of MSSP services over the next 24 months (see Figure 2). [2]

Figure 2. Managed Security Services Usage Change

How will your organization's use of managed security services change over the next 24 months? (Percent of respondents, N=251)

Decrease somewhat, 1%

Remain about the same, 13%

Increase substantially, 35%

Increase somewhat, 51%

Source: Enterprise Strategy Group, 2016

The services offered by MSSPs can help close the resource and skill set gaps by allowing organizations to offload tactical and operational tasks (e.g., 24x7 monitoring, writing firewall rules, and vulnerability management) and gain access to advanced skills and services such as incident response, situational awareness, and strategic risk mitigation planning. MSSPs that can leverage extensive telemetry across a broad set of customers to gather threat intel—a capability typically found only in network and telco providers—are uniquely positioned to provide contextual and actionable threat intelligence. Speed matters, and fast detection expedites the response to prevent incidents from becoming breaches and to reduce dwell time.

To offer this breadth of services across on-premises, hosted, and cloud infrastructures, managed security services providers must possess a range of skills and employ a platform to consolidate managed and co-managed offerings. This ESG Lab white paper explores how CenturyLink's new set of managed security services leverages a common platform to provide operational and advanced services to help customers execute on their cybersecurity initiatives.

CenturyLink Managed Security Services

CenturyLink is a global communication, hosting, cloud, and IT services company providing technology solutions to millions of customers worldwide. CenturyLink offers a broad portfolio of services including network and data systems management, big data analytics, IT consulting, and managed services. CenturyLink operates more than 55 data centers in North America, Europe, and Asia.

CenturyLink Managed Security Services (MSS) are designed to provide a unified complement of threat prevention, threat management, incident response, and forensic analysis services to support hosted, on-premises, and hybrid enterprise

---

[2] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

security environments. CenturyLink offers monitoring, management, and support across its entire security service offering, and provides customers with persistent visibility into their service information through a highly automated, online, self-service portal.

CenturyLink covers the entire IT stack with the goal of reducing the security and stability risks that come naturally when organizations try to manage and integrate disparate technologies, services, and SLAs across multiple vendors. This holistic approach provides multiple benefits to CenturyLink clients, including:

- **The CenturyLink Security Services Ecosystem**—CenturyLink MSS is designed to handle the entire attack lifecycle starting with preventative services such as distributed denial of service (DDoS) attack mitigation and managed firewalls, VPNs, and intrusion prevention systems (IPS), and advancing to proactive detection, containment, and incident response services that incorporate global threat intelligence, deep analytics, and security information and event management (SIEM) technologies to address a broad range of needs.

- **Expertise**—CenturyLink provides individualized consulting expertise and security operations center (SOC) professionals, along with solutions built using the same standards, processes, and threat intelligence that secure their millions of customers, global networks, and business assets. CenturyLink can evaluate organizations' regulatory environments, industries, geographies, risk profiles, business priorities, and security maturity, and then recommend a security program and practical services that most appropriately balance cost with actual risk.

- **Flexibility**—To address the individualized needs of different organizations, CenturyLink offers the ability to deliver security solutions alongside CenturyLink hosting, cloud, network, and colocation services. Services can be delivered as standalone offerings or to supplement existing services; fully managed or co-managed; and on-premises, hosted, or a hybrid mix. CenturyLink also offers flexibility in pricing, with consumption-based models on select services.

- **Visibility and Transparency**—Dashboards enable organizations to easily visualize their security postures, gaining insight into threat patterns and enabling more accurate decision making that leads to faster and more efficient incident response. Organizations may also use the dashboard to get visibility into real-time activity of the CenturyLink SOC in order to verify the work being done on the customer's behalf. Detailed reporting is provided to satisfy auditors and inform the board of directors.

- **Always-on Monitoring**—CenturyLink staffs 24x7 security operations centers to provide continuous monitoring and incident response. CenturyLink SOCs are staffed by more than 250 researchers, testers, and Global Information Assurance Certification (GIAC) holding intrusion analysts covering multiple security domains and holding multiple industry and vendor certifications including CISSP, CCNA, CCSP, CCSE, CCSA, and MCSE.

The CenturyLink MSS Portal is shown in Figure 3. The portal was designed with role-based access and workflows. The experience is different depending on the role of the user logging in. The portal was designed with usability top of mind. Customers have access and are provided with the ability to perform useful work with, and extract value from, their data.

Figure 3. CenturyLink Managed Security Services Portal

MSS Portal Dashboard View

Role-Based Workflows

Each circle in the portal is an item of interest, color-coded by severity and sized by probable impact; this design provides a user with an instant visualization of how her organization is being attacked from different regions. The objects on the dashboard are active and customizable.

The Economic Benefits of CenturyLink MSS

Enterprises and government entities are challenged to balance their specific business risks against their available—and often limited—resources and priorities. To effectively manage risk, organizations need to spend efficiently on cybersecurity. Assessing needs and setting priorities is crucial.

Before assessing risk, organizations must examine their assets carefully, with a goal of determining the acceptable level of risk for each asset. For example, revenue-generating assets will require higher levels of risk mitigation, and more funds should be allocated to protect them. Noncritical assets can assume higher risk and a smaller allocation of the security budget.

Once assets have been inventoried and evaluated, risk can be assessed and assigned to each. Key questions include: How vulnerable are those assets today? Are appropriate protections in place, i.e., identity and access management, encryption, and patching? Have critical vulnerabilities in those assets been identified and addressed? Assets with critical vulnerabilities must be prioritized in terms of security resources and efforts.

CenturyLink's MSS portfolio enables clients to leverage CenturyLink's security expertise so they can prioritize budget and resources around real risks and business goals. This guides them to subscribing to managed security services that leverage existing technology investments (e.g., existing SIEMs and security devices) to extract more value from them and obtain better ROI. The move from capital expenditures (CapEx) to operational expenditures (OpEx) transfers the cost of ownership to CenturyLink. Leveraging the economies of scale inherent in CenturyLink's global operations team provides greater operational efficiency than organizations can achieve on their own. CenturyLink's global visibility into threat intelligence across its own organization, its network, and all customer implementations provides better threat intelligence than organizations can hope to achieve independently. Finally, security as a managed service allows the flexibility of consumption-based pricing models and greater predictability of costs over time, which drives even more value.

Taken together, these features should enable an enterprise or government agency to improve its compliance-based and threat-focused security posture while controlling expenses by correctly prioritizing and focusing spending. By avoiding large new investments in technology and staff resources in favor of a predictable OpEx model that combines deep human knowledge and skill with advanced technology and automation, organizations can minimize their risks while optimizing their budgets.

A Customer's Perspective

ESG spoke with a cybersecurity director at a multinational consumer goods corporation who engaged CenturyLink as a strategic partner to help identify the company's most critical IT assets and to deploy global projects to secure those assets. Consumer data is the company's most critical information asset, and the organization decided to deploy the CIS Critical Security Controls (CIS Controls) for that environment as part of the cybersecurity framework. The CIS Controls are a prioritized set of actions for cyber defense that provide specific and actionable methods for addressing the most pervasive and dangerous attacks.

The data resided in a preexisting environment hosted by CenturyLink, which was responsible for the management of everything with the exception of the application. In this environment, the customer had engaged CenturyLink to deploy endpoint monitoring, host-based firewalls, and next-gen firewalls, along with SIEM and SOC services. The company engaged CenturyLink to prescribe capabilities and offerings from both its portfolio of standard services and customized offerings tailored to the organization, with the initial focus on alerting, monitoring, and logging. CenturyLink performed a thorough audit and assessment of the customer's critical assets, identifying and deploying the missing security controls and addressing critical vulnerabilities.

> "Century Link improved our ability to detect and automatically alert on specific use cases. Certain events related to security in the environment now have a more robust monitoring system in place to detect those," said the cybersecurity director, adding, "Aside from the application layer, CenturyLink owns the entire environment, so our security posture was improved—transparently to our users—with no impact to operations, no capital expense, and no additional in-house staff."

The company was able to shift budget away from less-critical assets to fund ongoing vulnerability scanning and management support of this complex environment. The customer's goal is to ensure 100% availability of the consumer data to internal users.

The customized offerings have created some "growing pains," but CenturyLink has been committed to delivering whatever the organization needs.

The cybersecurity director concluded: "They have all of the capabilities that we need to deliver the security posture that we have committed to our leadership, and if they don't currently have that capability they will find a way to make it happen. The advantage for us is that they manage our entire computing environment, and it's much easier when it's a one stop shop. We also use CenturyLink for cloud hosting. If you go to one of the leading cloud service providers and ask them to provide you with virtual compute services, manage those services, and provide managed security on top of those services, it's not something that's easy to obtain."

> "CenturyLink manages our entire computing environment...**and provides managed security.** It's much easier when it's a one stop shop."

The Bigger Truth

Cybersecurity initiatives were once again the most-cited IT priority for 2016, but an acute shortage of cybersecurity skills is limiting the ability of many organizations to implement those initiatives. In fact, 46% of participants in the same research conducted by ESG indicated that they have a problematic shortage of cybersecurity skills.[3] Organizations are further challenged to protect data assets that reside across on-premises, hosted, and cloud environments from compromise and ensure business continuity.

Security organizations must address two potentially conflicting objectives: increasing their organization's security posture while staying within allocated budgets and boosting operational efficiency. Extracting value from the investments organizations have already made in complex cybersecurity technologies is a daunting challenge. Platforms and services that integrate previously disparate technologies into streamlined workflows and incorporate shared services such as threat intelligence are needed.

MSSPs are playing an increasingly important role, enabling organizations to secure their assets and infrastructure with both operational services and strategic engagements. CenturyLink Managed Security Services are designed to provide a unified complement of threat prevention, threat management, incident response, and forensic analysis services to support hosted, on-premises, and hybrid enterprise and government security environments. CenturyLink offers monitoring, management, and support across its entire security service offering, and provides customers with persistent visibility into its service information through a highly automated, online, self-service portal.

The set of services offered by CenturyLink can close the resource and skills gaps by offloading tactical and operational tasks and providing access to advanced skills and services such as incident response, situational awareness, and strategic risk mitigation planning. CenturyLink leverages extensive telemetry across a broad set of customers and its network to offer contextual and actionable threat intelligence. Rapid detection shortens response time, which prevents incidents from becoming breaches.

ESG Lab performed a simple calculation to determine the economic benefit potential of CenturyLink MSS. The services we examined were CenturyLink's log monitoring service with 5 GB/day of data transfer and incident response services addressing three incidents per month. As of this writing, CenturyLink offers these services for $4,712 per month. Assuming a fully burdened cost of $150,000 for a skilled IT analyst, CenturyLink

CenturyLink can deliver Managed Security Services **at a 62% lower cost than hiring a full time employee.**

delivers these services at a 62% lower cost than hiring a new full time employee—assuming you can find one with the appropriate skill set.

CenturyLink covers the entire IT stack with the goal of reducing the security and stability risks that come naturally when organizations try to manage and integrate disparate technologies, services, and SLAs across multiple vendors.

If your organization is challenged by protecting your critical business assets—whether by a dearth of skilled security personnel, too much data to analyze, or a lack of 24x7 monitoring—and is spending more on cybersecurity yet still not satisfactorily addressing the risks, you should consider the economic and operational benefits of CenturyLink Managed Security Services. CenturyLink can help organizations balance costs against risk strategically and efficiently, focusing limited resources on the priorities with the greatest impact.

---

[3] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.